Public Key Infrastructure for the National Computational Science Alliance

(*the keys to the VMR*)

Randy Butler
Von Welch

National Computational Science Alliance

Presentation Outline

- **Alliance Secure Authentication Project**
  - **Background & Motivations**
  - **Process**
  - **Alliance PKI Components**
- **Grid Forum security activities**
- **MyProxy Key Management Service**

Alliance Computational Grid

- **Deploy standard infrastructure across Alliance sites.**
  - **Provide maximum capabilities to apps.**
  - **Increase what can be “taken for granted” when developing applications.**
  - **Reduce deployment burden at sites**
  - **Make it easy for new sites to join**

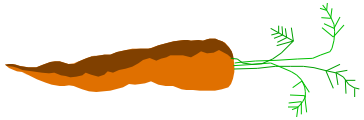
- **Alliance Computational Resources and Services (ACRS) sites**
  - **AHPCC, BU, MHPCC, NCSA, UKCC, UWisc**

Authentication Project Goals

- **Provide basis for grid security service**
- **Alliance identity for secure authentication**
- **Cross domain authentication**
- **Single sign-on**
- **Support grid applications *(API)***
- **Support grid services**
- **Scalable**
- **Interoperable *(don't mess up local site auth & acct mgt)***
- **Simple user interactions**
- **Extensible *(digital signatures encryption)***

Authentication Project Goals

- **Provide basis for grid security service**
- **Alliance identity for secure authentication**
- **Cross domain authentication**
- **Single sign-on**



- **Support grid applications *(API)***
- **Support grid services**
- **Scalable**
- **Interoperable *(don't mess up local site auth & acct mgt)***
- **Simple user interactions**
- **Extensible *(digital signatures encryption)***

R. Butler, NCSA (rbutler@ncsa.uiuc.edu)

Phase 1 Information Gathering

- **Surveyed ACRS site's authentication solutions**
  - **SSH – Kerberos – Unix Login**
- **Surveyed ACRS site's policies**
  - **none identified**
- **Proposed workshop to discuss Alliance strategy**
  - **ACRS sites policy and technical reps.**
  - **Technology developers (Globus team)**
  - **Security leads from other grid efforts**

Alliance Secure Authentication Workshop

- **Facilitator (Mark Bruhn)**
  - **Key to Workshop success!**
  - **Instrumental in early phases of the effort**
- **Proposed**
  - ✓ **Building an Alliance Public Key Infrastructure**
  - ✓ **Implementing via the Grid Security Infrastructure**
- **Adopted parallel tracks**
  - **Technical**
  - **Policy**
- **Agreed on the process**
  - **Task leads**
  - **Face-to-face &**
  - **Email discussions**

Technical Track

- Certificate Profile
  - Field population
  - Extensions
- Multiple CA acceptance
- Support for CRLs
- Mapping issues
- Software verification
- Platform support
- Error handling
- Administration tools
- Site specifics
- Enable policy requirements

Policy Track

- Alliance PKI Blueprint
- Modeled after the Federal PKI Working Group (FPKIWG) Model Certificate Policy (CP)
- Slogged through the document paragraph by paragraph, line by line.
- Process identified many technical requirements
- Required understanding of technical limitations

- Required leadership but not dictatorship

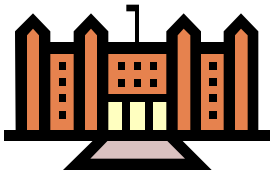
Related Alliance Activities

- Alliance Account Management Working Group
  - Allocations
  - ACRS site account administration groups
  - Allocations database
- Outreach
  - Documentation
  - Training
  - Promotion
  - Support
- Processes
  - Distinguished Names
  - Grid Mapfile Administration
  - Certificate Revocation
  - Identity Vetting
  - Credential Request/Retrieval

Basic Alliance PKI Components

- **Certificate Policy and Procedures**

- **Certificate & Registration Authorities**
  - **Certificate Generation Process**
  - **Distinguished Names**
  - **Registration**



- **PKI Administration and Support**
  - **Documentation**
  - **Grid Mapfiles**
  - **Revocation**
- **Grid Security Infrastructure Service**
  - **Certificate Request and Retrieval**
  - **Authentication Services**

Alliance PKI Certificate Creation Basics

R. Butler, NCSA (rbutler@ncsa.uiuc.edu)

Alliance PKI Certificate Creation Basics

Requestor Generates Key Pair
cert_request/browser

R. Butler, NCSA (rbutler@ncsa.uiuc.edu)

Alliance PKI Certificate Creation Basics

Requestor Generates Key Pair
cert_request/browser

Requestor Submits Public Key + ID to RA

R. Butler, NCSA (rbutler@ncsa.uiuc.edu)

Alliance PKI Certificate Creation Basics

Requestor Generates Key Pair
cert_request/browser

Requestor Submits Public Key + ID to RA

RA Verifies ID, Key Pair,
and User Eligibility

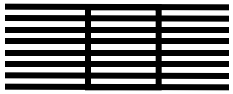
R. Butler, NCSA (rbutler@ncsa.uiuc.edu)

Alliance PKI Certificate Creation Basics

Requestor Generates Key Pair
cert_request/browser

Requestor Submits Public Key + ID to RA

Allocation Database



RA Verifies ID, Key Pair,
and User Eligibility

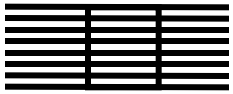
R. Butler, NCSA (rbutler@ncsa.uiuc.edu)

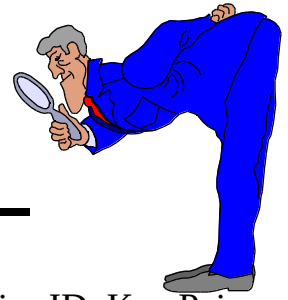
Alliance PKI Certificate Creation Basics

Requestor Generates Key Pair
cert_request/browser

Requestor Submits Public Key + ID to RA

Allocation Database





RA Verifies ID, Key Pair,
and User Eligibility

CA Binds Public Key to ID
by Signing the Certificate

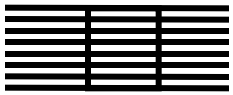
R. Butler, NCSA (rbutler@ncsa.uiuc.edu)

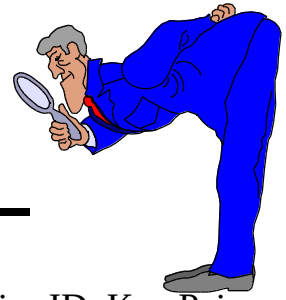
Alliance PKI Certificate Creation Basics

Requestor Generates Key Pair
cert_request/browser

Requestor Submits Public Key + ID to RA

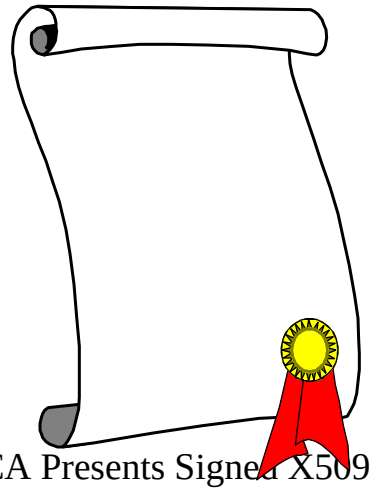
Allocation Database





RA Verifies ID, Key Pair,
and User Eligibility

CA Binds Public Key to ID
by Signing the Certificate



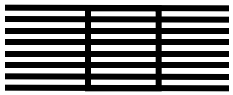
CA Presents Signed X509 v3
Certificate to Requestor

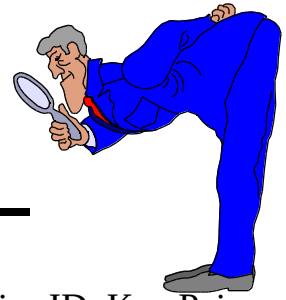
Alliance PKI Certificate Creation Basics

Requestor Generates Key Pair
cert_request/browser

Requestor Submits Public Key + ID to RA

Allocation Database

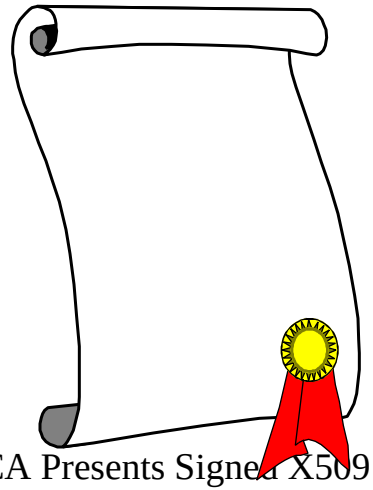




RA Verifies ID, Key Pair,
and User Eligibility

CA Binds Public Key to ID
by Signing the Certificate

Notify Acct Mgt



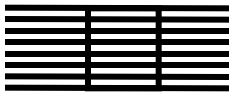
CA Presents Signed X509 v3
Certificate to Requestor

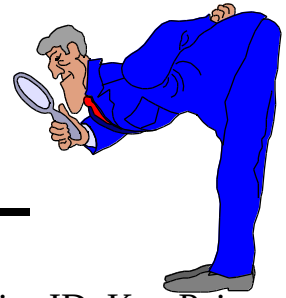
Alliance PKI Certificate Creation Basics

Requestor Generates Key Pair
cert_request/browser

Requestor Submits Public Key + ID to RA

Allocation Database

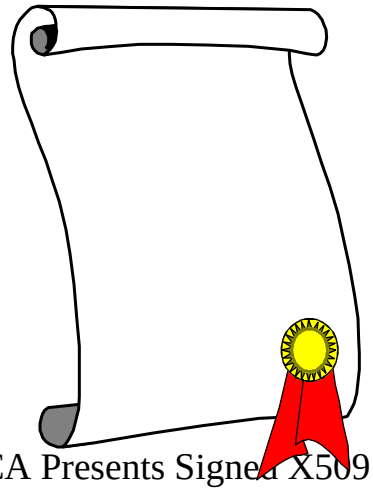




RA Verifies ID, Key Pair,
and User Eligibility

CA Binds Public Key to ID
by Signing the Certificate

Notify Acct Mgt



CA Presents Signed X509 v3
Certificate to Requestor

GSI Administration

- **Account Management System**
  - **Grid Mapfile Administration**
    - **Pushed from NCSA to ACRS sites**
  - **Certificate Revocations**
    - **Update of grid mapfile and CRL push**
  - **Distinguished Name Administration**
    - **Today Alliance DNs only**
- **Documentation**

Deployment and Testing

- **Early Users**
  - PKI deployment & support team
  - Eager applications developers
  - Globus certified users
  - Registration process

- **User Documentation**
  - Major effort documenting
    - Certificate process
    - GSI
    - admin

Production

- Couple thousand certificates
- Registration process
  - Registration models (You get what you pay for!)
    - Classic PKI user verification
    - Streamlined verification
- Replace local account access*
- Cross certification issues
- Key Management
- Long Term CA thoughts

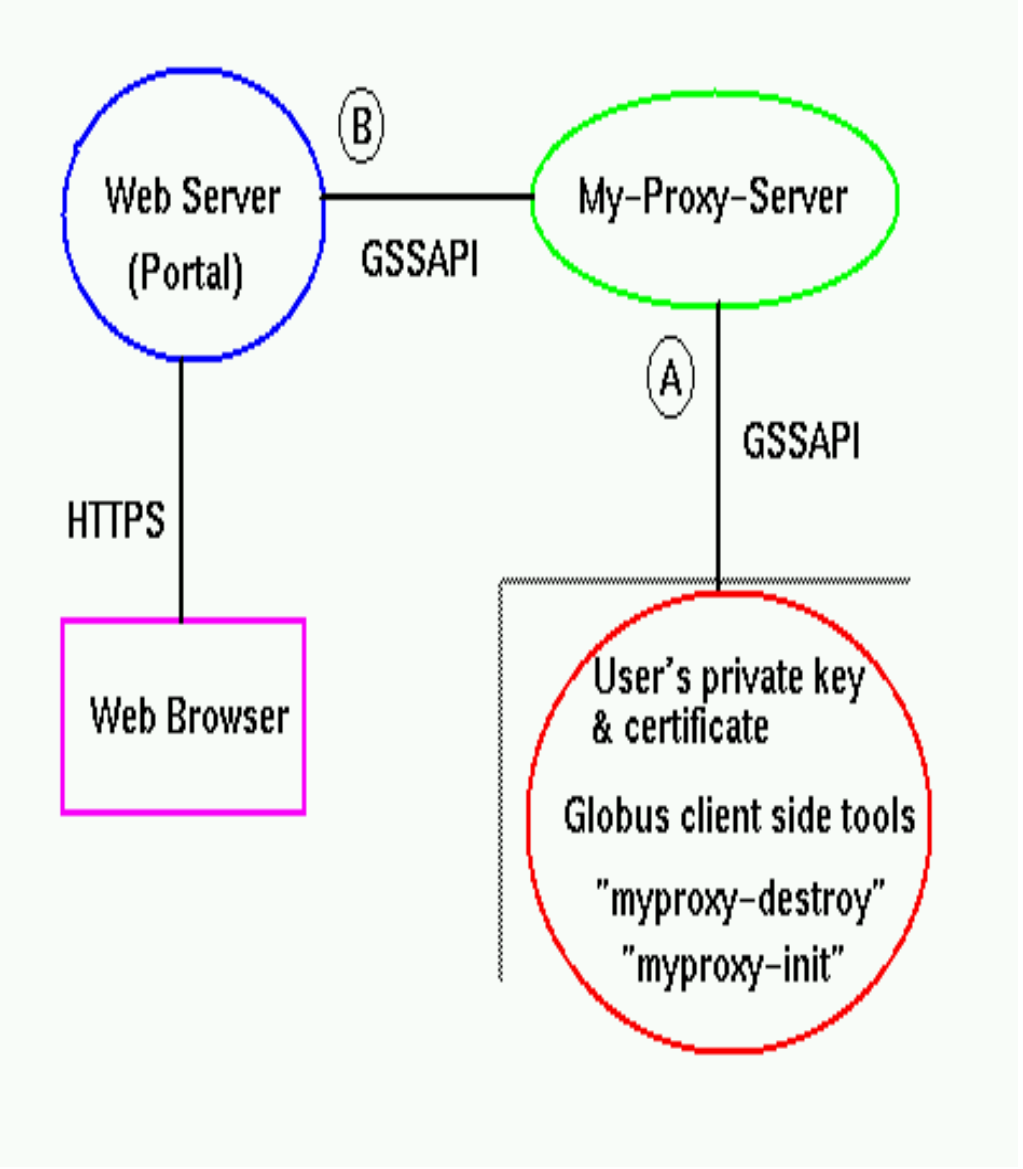
GridForum related activities

- GSI effort lead by Steve Tuecke & Marty Humphrey
  - Identify Grid Security Requirements
  - Map to or extend GSI
- Certificate Policy effort lead by Randy Butler and John Volmer
  - Identify Grid Policy Requirements
  - Lead to a Grid Certificate Policy Model
    - So “we” can more readily exchange certificates without closing our eyes
    - To act as a blueprint for new Grid PKIs

Alliance Key Management Research

MyProxy Security Delegation Service
Driven by Alliance Science Portals

- **One thing that differentiates a portal from a web page is its ability to do work on behalf of the user.**
- **This however requires some sort of delegation.**
- **MyProxy was developed to "securely" serve this need.**



R. Butler, NCSA (rbutler@ncsa.uiuc.edu)

PKI Key Management Issues

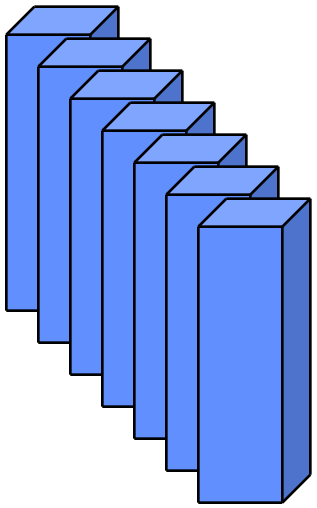
- **Challenging for users**
  - **Install private key and cert on every “from’ host**
  - **Vulnerable when left on a “foreign” host**
  - **Which certificate when, etc…….**
- **Concerning for security administrators**
  - **Users will look for short cuts**
  - **Users likely won’t appreciate vulnerabilities**

Extending MyProxy

- **Why not use MyProxy to securely manage the user's private key and X509 certificate?**
- **Akin to a Kerberos Key Distribution Center (KDC)**

Model #1: MyProxy Key Management

Delivers proxy to user

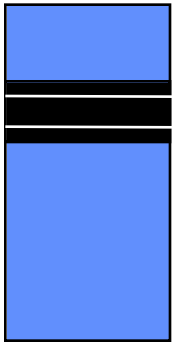


Resource

③ User authenticates with proxy

• User registration
Pass Phrase + UID

② Proxy



MyProxy

Model #2: MyProxy Delegation Cache

2. UID + PP'

Portal

Stores proxy
Delivers proxy to portal

3.2 Proxy'

3.1 UID + PP'

1.1 Registration UID + PP

1.2 MPS Store Proxy PP'

MyProxy

R. Butler, NCSA (rbutler@ncsa.uiuc.edu)

More Information

National Computational Science Alliance

http://www.ncsa.uiuc.edu

Virtual Machine Room

http://www.ncsa.uiuc.edu/SCD/Alliance/VMR

Globus Project

http://www.globus.org

My Proxy

http://www.dast.nlanr.net/Features/MyProxy/